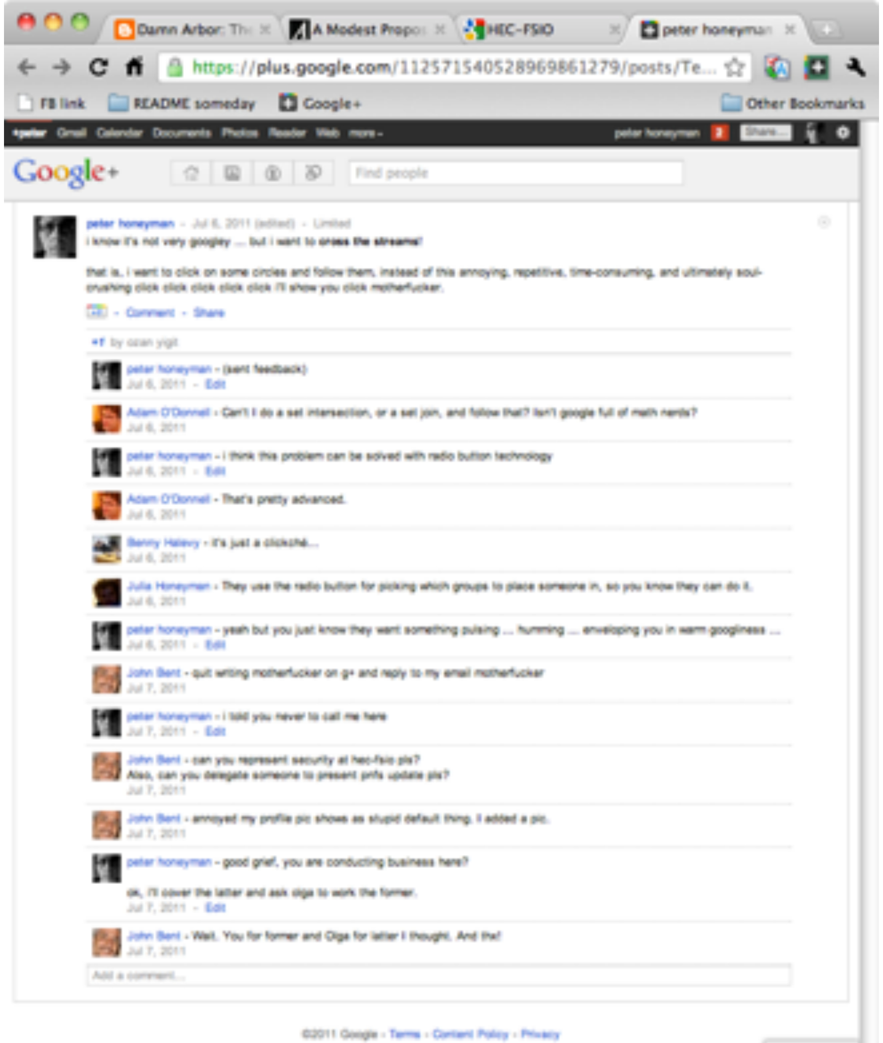
Security

Peter Honeyman
CITI, University of Michigan

Important business ...



peter honeyman - Jul 6, 2011 (edited) - Limited
i know it's not very googley ... but i want to cross the streams!

that is, i want to click on some circles and follow them, instead of this annoying, repetitive, time-consuming, and ultimately soul-crushing click click click click click i'll show you click motherfucker.

+1 - Comment - Share

+1 by ozan yigit

peter honeyman - (sent feedback)
Jul 6, 2011 - Edit

Adam O'Donnell - Can't I do a set intersection, or a set join, and follow that? Isn't google full of math nerds?
Jul 6, 2011

peter honeyman - i think this problem can be solved with radio button technology
Jul 6, 2011 - Edit

Adam O'Donnell - That's pretty advanced.
Jul 6, 2011

Benny Halevy - it's just a clickché...
Jul 6, 2011

Julia Honeyman - They use the radio button for picking which groups to place someone in, so you know they can do it.
Jul 6, 2011

peter honeyman - yeah but you just know they want something pulsing ... humming ... enveloping you in warm googliness ...
Jul 6, 2011 - Edit

John Bent - quit writing motherfucker on g+ and reply to my email motherfucker
Jul 7, 2011

peter honeyman - i told you never to call me here
Jul 7, 2011 - Edit

John Bent - can you represent security at hec-fsio pls?
Also, can you delegate someone to present pnfs update pls?
Jul 7, 2011

John Bent - annoyed my profile pic shows as stupid default thing. I added a pic.
Jul 7, 2011

peter honeyman - good grief, you are conducting business here?

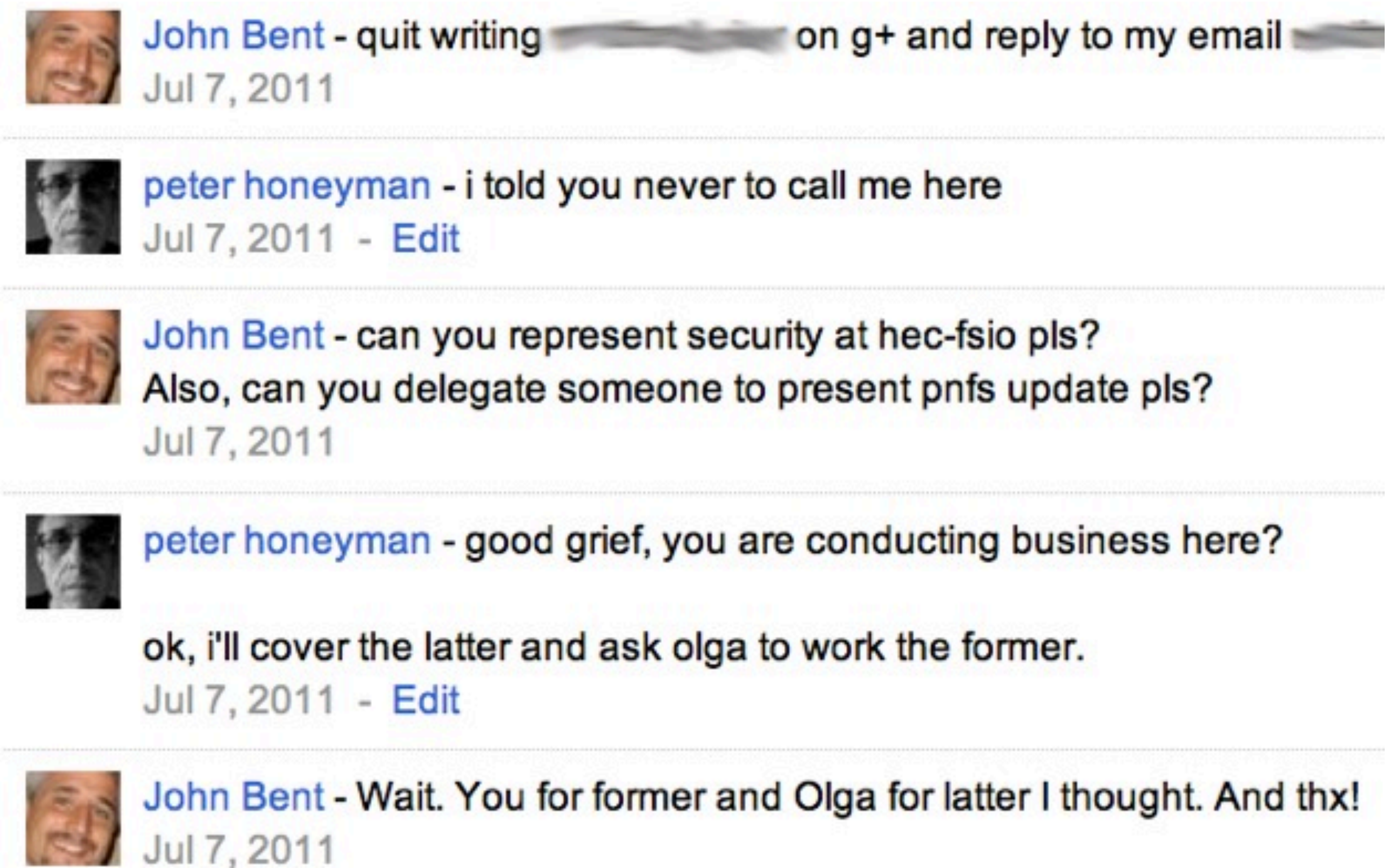
ok, i'll cover the latter and ask olga to work the former.
Jul 7, 2011 - Edit

John Bent - Wait. You for former and Olga for latter I thought. And tha!
Jul 7, 2011

Add a comment...

©2011 Google - Terms - Content Policy - Privacy

… without boundaries



John Bent - quit writing [redacted] on g+ and reply to my email [redacted]
Jul 7, 2011

peter honeyman - i told you never to call me here
Jul 7, 2011 - Edit

John Bent - can you represent security at hec-fsio pls?
Also, can you delegate someone to present pnfs update pls?
Jul 7, 2011

peter honeyman - good grief, you are conducting business here?

ok, i'll cover the latter and ask olga to work the former.
Jul 7, 2011 - Edit

John Bent - Wait. You for former and Olga for latter I thought. And thx!
Jul 7, 2011

My research insecurity

- Click to add text
    - Thanks a lot, Dr. Bent

Early NFS security

- IP address-based authentication for mounting
- RPC security flavors
    - AUTH_NONE
        - Null credential
    - AUTH_SYS
        - Trusted client
- Easily guessed file handles

NFSv3 security

- Random initial generation number
- AUTH_DES / AUTH_DH
- AUTH_KERB4
    - Not widely supported
- NFSv4 brought along RPCSEC_GSS for NFSv3
- Network name issues

NFSv4 security

- GSS-API the ultimate RPC security flavor
    - Kerberos V mandatory
    - PK FAIL
        - PKInit helps some, PKU2U has some fans
        - NFSv4 security w/o Kerberos? I doubt it.
- ACLs: NFSv4 vs. POSIX vs. Microsoft

NFSv4.1 security

- Sessions
    - Avoids conflict between multiple users and exactly-once semantics
- State protection with SSV
    - Avoids problems with multiple users when no machine cred
- Back channel (callback) protection

pNFS security

- File: not much difference
- Object: much difference
- Block: what’s the difference?

Labeled NFS

- Client attaches security attribute of the requesting subject
    - RPCSEC_GSS.v3 protocol change
- Object labels
    - NFSv4.2 protocol change
    - Store as **`recommended attribute`**
        - **`named attribute`** not atomically set on creation, stored as FS object itself

Labeled NFS

- Opaque object label is attached at creation (OPEN, CREATE)
- Callback for label change notification
- Added to NFSv4.2 charter
- Might play a role in provenance tracking

Some challenges

- Key management
  - Plutus (FAST ’03) is clever and fast
- GSS scaling in large clusters
  - E.g., 10,000 storage servers want Kerberos tickets ...
- Credential translation and management
  - Complementary security assertions in PK and Kerberos